ESC-TR-98-043

Quarterly Technical Summary

Advanced Electronics Technology

15 November 1998

Lincoln Laboratory

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LEXINGTON, MASSACHUSETTS

Prepared for the Department of the Air Force under Contract F19628-95-C-0002.

This report is based on studies performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. The work was sponsored by the Department of the Air Force under Contract F19628-95-C-0002.

The ESC Public Affairs Office has reviewed this report, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

Gary Tutungian
Administrative Contracting Officer
Contracted Support Management

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

ADVANCED ELECTRONICS TECHNOLOGY

QUARTERLY TECHNICAL SUMMARY REPORT
TO THE
AIR FORCE MATERIEL COMMAND

1 AUGUST – 31 OCTOBER 1998

ISSUED 22 FEBRUARY 1999

LEXINGTON MASSACHUSETTS

INTRODUCTION

This Quarterly Technical Summary covers the period 1 August through 31 October 1998. It consolidates the reports of Division 6 (Communications and Information Technology) and Division 8 (Solid State) on the Advanced Electronics Technology Program.

TABLE OF CONTENTS

COMMUNICATIONS AND INFORMATION TECHNOLOGY
DIVISION 6

INTRODUCTION

This section of the report reviews progress on Machine Intelligence Technology during the period 1 August through 31 October 1998. Separate reports describing other Information Systems Technology work of Division 6 are issued for the following programs:

Tactical Speech Technology	AFRL/IFEC
Speech and Signal Processing Technology	NSA

V. W. Chan
Head, Division 6

C. W. Niessen
Associate Head

MACHINE INTELLIGENCE TECHNOLOGY
GROUP 62

1. INTRODUCTION

The objective of the Machine Intelligence Program has been the application of MI techniques to problems in the interpretation and utilization of data produced by imaging sensors. Past emphasis has been on algorithms for ISAR (Inverse Synthetic Array Radar) and SAR (Synthetic Array Radar) imaging sensors and on processors for real-time, fully- automated applications such as automatic recognition of re-entry vehicles (the ISAR application) and of ground vehicles (the SAR application). The image understanding application emphasis has been shifted over the past 18 months to concentrate on exploitation technology for visible and IR multispectral sensors, most particularly night vision research in which low-light visible and IR images are combined to create a color night vision capability. Fusion techniques have also been applied to image enhancement and color display algorithm development to facilitate analyst-based exploitation of multispectral surveillance images, and to multispectral surveillance algorithm research to develop automatic target detection algorithms for operation in complex environments. The line-supported work on night vision was completed last FY, with follow-on work on algorithms, real-time implementation, and low-light CCD sensor technology being funded by DARPA.

Motivated by the growing vulnerability of large-scale military and national information-dependent infrastructure systems to exploitation, manipulation, and sabotage, Lincoln Laboratory conducted a study during FY95 commissioned by DARPA/ITO. The study goal was to recommend technical approaches and technology-based strategies to address this situation, particularly in regard to current and future U.S. Military Command, Control, Communications, Computers, and Intelligence (C4I) systems. Also in the FY95-96 time frame, Lincoln participated in several national studies focused on these issues, including the DARPA Information Science and Technology FY95 summer study on Defensive Information Warfare, and the FY96 Defense Science Board Task Force on Defensive Information Warfare (IW-D). As an outgrowth of these efforts, Lincoln initiated in FY97 an OSD Line-supported IW-D technology development program focused on the following major aspects of this important national security problem:

- Survivable Distributed C4I Systems
- Computer/Network Monitoring and Surveillance

Work in these two areas during the third quarter of FY98 is summarized below.

2. SURVIVABLE DISTRIBUTED C4I

We have continued to develop a test bed for measuring the performance of multicast applications. We have developed automated scripts that can monitor CPU utilization and network activity on each host. CPU utilization information is sampled every five seconds and recorded to a log file. Every

network packet sent or received, along with precise timing information, is also recorded to a log file. By analyzing the log files we can derive bandwidth utilization, throughput, packet loss rates, and other information.

To evaluate this measurement system, and to be sure that our monitoring activity does not interfere with the application being measured, we have collected data on a secure video multicast application. We chose this application because it requires significant CPU and network resources, leaving few resources available for the monitoring activity. If the monitoring were to consume excessive CPU resources, then we would expect to see an effect in the video application or missing data samples in the log files. In our preliminary measurements, this does not seem to be a problem.

We have begun to implement scripts that will analyze the raw data in the network log files. We plan to have the scripts generate plots that show how throughput and loss rates change over time. This is important for applications that produce data at a variable rate and for wireless network links that have time varying characteristics.

We plan to use this measurement system to make detailed measurements of the behavior of reliable multicast protocols in the presence of denial-of-service attacks. We plan to measure the performance of the protocols in a benign environment, and then expect to see a noticeable change when an attack is launched. We also hope to see a noticeable improvement when we apply security and survivability measures to the protocols.

3. COMPUTER/NETWORK MONITORING AND SURVEILLANCE

3.1 Overview

Lincoln is in the midst of coordinating the first quantitative and repeatable evaluation of intrusion detection systems. During the past quarter, we have used our simulation test bed to generate an additional two weeks' worth of network traffic and audit log files. These data, containing normal network traffic mixed with attack traffic, have been distributed to seven government contractors who will use the data to evaluate their computer network intrusion detection systems. These data supplement the seven weeks of training data previously generated and distributed.

During the past quarter, we made significant progress towards making our simulation more realistic by incorporating human actors. This work is described in Section 3.2.

3.2 Actor-Based Traffic Generation for Intrusion Detection Evaluation

We use a simulated Air Force base TCP/IP network and a simulated external Internet to generate data for the testing and evaluation of intrusion detection systems. This simulation runs on a mixed network of Solaris, SunOS and Linux workstations. Because the simulation runs in real time, simulates hundreds of hosts and users, and uses only a small number of machines to represent the entire network, it is possible for someone in the real world to directly interact with the simulation. This property was used to greatly enhance the ability of the simulation to represent real world interactions between humans, and to provide a more realistic model of the types and duration of the network traffic that would appear on a real-world network.

These workstations are used to generate network traffic in a wide range of types and duration, and in a manner that is statistically similar to the real-world traffic that would be found on a typical Air Force base. Most of this traffic is generated using Perl scripts, which have been written and tested in advance. Each script is written in such a way that the traffic that it generates appears to be coming from a single simulated user. Simulated accounts and password files, for the virtual users on the traffic generation machines, are used to ensure that the virtual users are able to perform the same actions that real world users would be able to, including logging in to other machines remotely, sending and receiving e-mail, running processes, and so on. In addition to typical network activity, scripted network attacks are also generated by these Perl scripts. Some forms of attacks are also run by hand.

To create the illusion of having a large number of unique hosts on the network, a kernel modification called FakeIP is used on the Linux host network traffic generators. This modification makes it possible for the network traffic which originates on those machines to appear to originate at a virtual host with an IP address and hostname that are different from the IP address and hostname of the machine on which the traffic is actually originating. This also ensures that when replies are sent to incoming traffic from virtual hosts, that the replies will be sent to the correct virtual machine, instead of the physical host that actually sent the data.

Unfortunately, if all of the network activity in the simulation is automated, then the simulation either loses a great deal of realism, or it becomes prohibitively complicated to operate the simulation. For example, certain system administrative activities are too complicated to simulate using scripts. Some of these activities, such as adding users to password files, compiling complex applications, and updating software on workstations do not lend themselves well to being executed through a Perl script. In addition, other kinds of activities, such as web browsing or running other graphical applications which require the use of a mouse, are extremely difficult to simulate. Furthermore, some forms of human behavior, such as making typos, varying typing speed and patterns in a realistic manner, and forgetting to run or stop running processes when needed, are also very difficult to simulate. The problem is complicated further by the fact that some of the attacks that are run during the simulation must be run by hand. This would make these attacks very easy to detect if the only other traffic on the network is automated.

To solve these problems, and to add network traffic on infrequently used services, human interaction with the network is required. Having real humans interact with the simulation makes it possible to run X (graphical) applications easily without complicated scripting. It puts an intelligence behind some of the network activity, which makes the network traffic appear to be more realistic. Plus, human interaction prevents hand-run attacks from being trivial to identify, because there is non-attack related traffic on the network as well.

Human interaction with the simulation was implemented by assigning a real world human to perform as a "human actor." A human actor is responsible for assuming the identity of a variety of virtual humans in the simulation, and behaving on the network in a manner which is consistent with the role that the virtual human has in the simulation. The actor simulates the actions of three remote system administrators, a local console-based administrator, and a number of non-privileged users. These actions are run during the day, starting at 8 AM simulation time, and ending whenever the real world human has

to leave for the day. Actions are recorded as they happen using the UNIX script command, and are also recorded by hand on paper. Recorded events are later transferred to the Group 62 network for analysis.

Each of the three system administrators was given a profile to determine how they would behave during the simulation. The "Simple" system administrator was a person who knew how to perform regular administrative duties, but who could not do anything that was more sophisticated. He handled e-mail from users, monitored system logs, and performed software maintenance duties. He was also responsible for adding and removing users. Because of his inexperience, however, the simple administrator was not security savvy, and made many mistakes.

The "Smart" administrator was a more sophisticated, more experienced system administrator. She was on call for more complicated tasks, but because of her experience, she was often in demand by other sites, and usually only did work for the base for an hour or two each day. Her duties included handling difficult system maintenance tasks, performing network related tasks, handling problems that the other system administrators were not capable of fixing, writing code, and running long-term CPU intensive jobs.

Finally, the Web/FTP administrator was responsible for the maintenance of the base Web and FTP sites. His duties included the design of new web pages, checking the logs of the web server, and performing other Web and FTP site related activities. To check his work, he frequently remote-displayed Netscape to his workstation on the outside network, and browsed the internal base website. He performed site updates one to two times per day to reflect updated base news and weather information.

A variety of steps are taken during the simulation to ensure that the set of actions taken by the virtual humans who are being simulated by the human actor are performed in as realistic a manner as possible. For example, actions from different users and administrators are mixed together to provide the illusion of many different people working on the network at once, and are timed to make it appear that in addition to their network-based activities, the virtual users are also responding to events in the real world around them.

Maintaining the right mix of actions for each virtual human also requires that each virtual human is able to run a mix of processes and perform a set of activities that not only change in a realistic manner, but which also maintain a realistic mix of different network activities. The activities which are simulated include standard system administration activities, e-mail (SMTP and IMAP), web browsing (HTTP), remote display of X applications (X11), FTP, IRC, and network administration activities such as ping, as well as the creation, compilation and execution of code.

Because many system administration related activities involve the same actions, services, and programs that are used by attackers, certain activities are chosen specifically to test whether or not an intrusion detection system will generate false alarms. These include running long-term jobs, looking through system directories, editing system logs, running ping and crack, jumping from system to system, running sniffers such as TCPdump, obtaining root access, and compiling and installing new software.

Many programs are downloaded by the virtual system administrators from a simulated FTP server. The programs are placed on the virtual FTP server during simulation down time, and are then run during the day as regular human actions. The mix of these programs is designed to reflect the wide variety of tasks and interests for which real humans choose software. These programs included MASH (a

networked whiteboarding program), Maelstrom (a game), an IRC client (for on line chatting), LNKnet (a Lincoln Laboratory research application), and Microsoft Internet Explorer 4 for Solaris (a web browser). Installation of these programs was sometimes performed at the request of virtual non-privileged users, and at other times because the virtual system administrators needed them for their work.

Other programs were preinstalled on some of the Linux machines on the network. These were also run to reflect real-world activities, and to generate X11 network activity. For example, The Gimp (an open source image manipulation program that is similar to Adobe Photoshop) was run by the "Simple" administrator to evaluate its potential for base users, and by the web administrator for use in the creation of images for the base website. All of the administrators ran Netscape for web browsing. XV (an X-based image viewer) was also used for viewing various images and postscript files.

Unfortunately, having real humans interacting with the simulation created a problem with maintaining the illusion of a real network. On some of the simulation machines, normal system administration activities, such as running top, ps, or who, could have revealed that users and processes that were supposedly running on a large number of machines were actually all being run on a single host. Simulation specific configurations such as password files and simulation files could have given away simulation details. Other details, such as the names and times of attacks could also have been revealed.

To avoid this problem, a number of "no-name" machines were set up on the *SimNet*. A no-name machine is a Linux workstation with the ability to take on the identity of a virtual host. The virtual host essentially becomes a real, physical machine, and all traffic intended to go to the virtual host is redirected to the no-name machine. The advantage to doing this is that no details of the simulation are present on a no-name machine and, therefore, running processes on a no-name machine will not give away the details of the simulation.

However, using a no-name machine does have a side effect. When the no-name machine assumes the identity of a virtual machine, scripts that were intended to run on that virtual machine are no longer able to run. This means that various scripted user activities and attacks were disabled while a no-name machine was active. To solve this problem, a simulated base internal Linux network was created, which was made up of ten virtual hosts. No scripts were permitted to run on any of these virtual hosts. So, if the no-name machines were used, they became a host which was not being used for anything, thus preventing disruptions to the simulation.

During the simulation, all of the human actor events are recorded on paper. The time at which the event starts, the source and destination network machines, and a description of the event are all recorded. The events are then identified by hand in lists of network data, and labeled as human actor events. The list files in which the events are located contain date, time, service, attack, and connection information for each network connection made in the simulation. The list files are used for the scoring of intrusion detection systems, verifying simulated network traffic, and verifying that human actor events were run properly.

Human actor events are important to the Intrusion Detection Evaluation simulation because they improve the realism of the simulation, and because they are used to generate data which is used to test the accuracy of intrusion detection systems. They make it simple to produce normal network activity that can not be automated easily. However, performing human activities on the network during a live simulation requires a great deal of extra care, since typing the wrong command or interacting with the

simulation in the wrong way could potentially destroy the illusion that the *SimNet* is actually a real Air Force base network.

SOLID STATE
DIVISION 8

INTRODUCTION

This section of the report summarizes progress during the period 1 August through 31 October 1998. The Solid State Research Report for the same period describes the work of Division 8 in more detail. Funding is provided by several DoD organizations—including the Air Force, Army, BMDO, DARPA, Navy, NSA, and OSD—and also by the DOE, NASA, and NIST.

D. C. Shaver
Head, Division 8

R. W. Ralston
Associate Head

DIVISION 8 REPORTS
ON ADVANCED ELECTRONICS TECHNOLOGY

1 AUGUST THROUGH 31 OCTOBER 1998

PUBLICATIONS

Silicon-Rich-Methacrylate Bilayer Resist for 193-nm Lithography	A. J. Blakeney* A. H. Gabor* D. White* T. Sternhäsler* W. R. Deady J. J. Jarmalowicz R. R. Kunz K. R. Dean* G. K. Rich* D. Shark*	*Solid State Technol.* **41**(6), 69 (1998)
Terahertz Photomixing in Low-Temperature-Grown GaAs	E. R. Brown S. Verghese K. A. McIntosh	*Proc. SPIE* **3357**, 132 (1998)
Low-Loss High-Efficiency and High-Power Diode-Pumped Mid-Infrared GaInSb/InAs Quantum Well Lasers	H. Q. Le C. H. Lin* S. S. Pei*	*Appl. Phys. Lett.* **72**, 3434 (1998)

ACCEPTED FOR PUBLICATION

Growth and Morphology of Er-Doped GaN on Sapphire and HVPE Substrates	R. J. Molnar R. Birkhahn* R. Hudgins* D. Lee* A. J. Steckl* J. M. Zavada*	*J. Vac. Sci. Technol.*

*Author not at Lincoln Laboratory.

Annealing Studies on GaN Hydride Vapor Phase Epitaxial Layers	R. J. Molnar D. C. Reynolds* D. C. Look* T. Wille K. K. Bajaj T. C. Collins	*Appl. Phys. Lett.*
Approaches to Designing Thermally Stable Schottky Contacts to *n*-GaN	R. J. Molnar H. S. Venugopalan* S. E. Mohney* J. M. DeLucca*	*Semicond. Sci. Technol.*
Rapid Evaluation of Dislocation Density in *n*-type GaN Films Using Photoenhanced Wet Etching	R. J. Molnar C. Youtsey* I. Adesida* L. T. Romano*	*Appl. Phys. Lett.*
A Photomixer Local Oscillator for a 630 GHz Heterodyne Receiver	S. Verghese K. A. McIntosh S. M. Duffy S. D. Calawa E. K. Duerr* D-Y. E. Tong* R. Kimberk* R. Blundell*	*Appl. Phys. Lett.*
InAs Doped Silica Films for Saturable Absorber Applications	J. N. Walpole L. J. Missaggia I. P. Bilinsky* J. G. Fujimoto*	*Appl. Phys. Lett.*

PRESENTATIONS†

Photonic A/D Converters for Wideband and High Dynamic Range Performance	J. C. Twichell Z. J. Lemnios C. Dickerson*	7th Annual AIAA/BMDO Technical Readiness Conference, Colorado Springs, Colorado, 3-7 August 1998

*Author not at Lincoln Laboratory.

†Titles of presentations are listed for information only. No copies are available for distribution.

Transmit Filters for Wireless Basestations	A. C. Anderson H. Wu* Z. Ma* P. A. Polakos* P. M. Mankiewich* T. Kaplan* A. Barfknecht*	Applied Superconductivity Conference, Palm Desert, California, 13-18 September 1998
Low-T_c Superconductive Circuits Fabricated on 150-mm Diameter Wafers by Using a Doubly Planarized Nb/AlO_x/Nb Process	K. K. Berggren D. A. Feld J. P. Sage E. M. Macedo	
Evaluation of Electrical Characteristics of Nb/Al/AlO_x/Nb Josephson Junctions Using Test Structures at 300 K	K. K. Berggren J. P. Sage A. H. Worsham* M. O'Hara*	
Measurements of the Energy Sensitivity of a Superconductive Comparator	D. A. Feld J. P. Sage K. K. Berggren A. Siddiqui*	
Magnetically Tunable Superconducting Resonators and Filters	D. E. Oates G. F. Dionne	
Measurements and Modeling of Microwave Impedance High-T_c Grain Boundaries	D. E. Oates Y. M. Habib* C. J. Lehner* L. R. Vale* R. H. Ono* G. Dresselhaus* M. Dresselhaus*	
First Demonstration of Correlation in a Niobum Superconductive Programmable Binary-Analog Matched Filter	J. P. Sage D. A. Feld	

*Author not at Lincoln Laboratory.

Passively Q-Switched Microchip Lasers and Applications	J. J. Zayhowski	European Conference on Lasers and Electro-Optics/ European Quantum Electronics Conference, Glasgow, Scotland, 13-18 September 1998
Dose Control Errors from Transient Absorption in Fused Silica	A. Grenville V. Liberman M. Rothschild J. H. C. Sedlacek A. K. Bates	
Photoresist Outgassing at 193 nm	R. R. Kunz D. K. Downs	
Damage Assessment of Optical Materials after Long-Term Irradiation	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro	4th International Symposium on 193-nm Lithography, Tyrol, Austria, 14-17 September 1998
Marathon Irradiation Testing of Antireflection and High Reflector Coatings for 193-nm Lithography	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro A. K. Bates C. VanPeski	
Do Top-Surface Imaged Silylation Resists Really Offer Performance Advantages?	S. C. Palmateer S. G. Cann J. E. Curtin S. Deneault A. Forte R. R. Kunz T. M. Lyszczarz C. Nelson M. B. Stern	

Damage Assessment of Pellicles for 193 nm Lithography	C. VanPeski A. K. Bates V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro	4th International Symposium on 193-nm Lithography, Tyrol, Austria, 14-17 September 1998
Critical Issues for Projection Lithography at 157 nm	T. M. Bloomstein M. Rothschild R. R. Kunz D. E. Hardy R. B. Goodman S. T. Palmacci	Mask Users Group Symposium, Berkeley, California, 15 September 1998
Summary of Round Robin 1 Results	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro	Fused Silica Workshop, Tyrol, Austria, 17 September 1998
Antimonide-Based Diode and Optically Pumped Mid-Infrared Lasers	H. K. Choi G. W. Turner H. Q. Le J. N. Walpole M. J. Manfra M. K. Connors L. J. Missaggia	Workshop on Middle Infrared Coherent Sources, Corsica, France, 22-26 September 1998
Marathon Testing of Optical Materials for 193-nm Lithographic Applications	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro A. K. Bates C. VanPeski	Annual Symposium on Optical Materials for High-Power Lasers, Boulder, Colorado, 28 September–2 October 1998
Current Status of Mid-Infrared Semiconductor Lasers	H. K. Choi	Optical Society of America Annual Meeting, Baltimore, Maryland, 4-9 October 1998

Extending the Cutoff Wavelength of Lattice-Matched GaInAsSb/GaSb Thermophotovoltaic Devices	C. A. Wang D. C. Oakley H. K. Choi	4th National Renewable Energy Laboratory Conference on Thermo-photovoltaic Generation of Electricity, Denver, Colorado, 11-14 October 1998
A Deep Submicrometer Fully-Depleted Low Power SOI CMOS Process Technology	J. A. Burns	Lincoln Laboratory Technical Seminar Series, University of Michigan, Ann Arbor, Michigan, 30 October 1998

SOLID STATE
DIVISION 8

1. QUANTUM ELECTRONICS

The thermal expansion coefficient and *dn/dT* have been measured in undoped YAG below 300 K using interferometry techniques. The thermal expansion coefficient at 125 K was 2.70×10^{-6} K^{-1} and *dn/dT* at 633 nm was 2.5×10^{-6} K^{-1}, compared with 7×10^{-6} K^{-1} and 9×10^{-6} K^{-1} for these quantities at 300 K.

2. ELECTRO-OPTICAL MATERIALS AND DEVICES

A ring laser using a tapered GaInAsP/InP amplifier as the gain element has provided 80-mW single-frequency output in a single-mode fiber. The fiber ring contains a tunable Fabry-Perot filter and a fiber Bragg grating to select a single mode of the ring.

The suitability of the wavelength range provided by silicon photodiode detector arrays for monitoring the spectral reflectance during epitaxial growth of GaSb, AlGaAsSb, and GaInAsSb has been demonstrated. By using a virtual interface model, the growth rate and complex refractive index at the growth temperature have been extracted for these alloys over the 600–1000-nm spectral range.

The optical characteristics of epitaxial GaInAsSb, a material for thermophotovoltaics, have been evaluated by photoluminescence. For these layers grown lattice matched to GaSb substrates by organometallic vapor phase epitaxy, the optical quality is improved as the growth temperature is lowered from 575 to 525°C.

3. SUBMICROMETER TECHNOLOGY

The chemical components released during 193-nm-wavelength exposure of photoresists have been analyzed, and a model has been developed to predict the effects of these chemicals on optical elements. This technique has been used to compare the long-term effects of using various resists in an optical exposure system.

4. BIOSENSOR AND MOLECULAR TECHNOLOGIES

A novel sensor is being developed which uses live cells integrated with microelectronics in order to identify pathogenic bacteria and viruses in a rapid, sensitive fashion. The feasibility of this approach has been proven by creating suitable genetically engineered cells, by demonstrating that their responses are very fast, sensitive, and specific, and by fabricating prototype hardware for the sensor.

5. MICROELECTRONICS

Attempts have been made to deform imager arrays to take advantage of the improved optical response of a curved focal surface compared to a planar one. A petal chip approach has been used to successfully deform a thinned Si membrane to a spherical surface with a 39-mm radius of curvature.

6. ANALOG DEVICE TECHNOLOGY

The energy sensitivity S_ε of a superconductive comparator has been measured to be about 1500 h (Planck's constant) when the comparator was clocked at 40 MHz, and the noise floor was low enough that we could observe excess low-frequency noise below 5 Hz. If we clock the comparator into the gigahertz range it may be possible to operate it with $S_\varepsilon = h$, the energy uncertainty principle limit.

7. ADVANCED SILICON TECHNOLOGY

The high-frequency performance of 0.25-μm channel length n- and p-channel metal-oxide semiconductor field-effect transistors (MOSFETs), developed as part of Lincoln Laboratory's fully depleted silicon-on-insulator CMOS process technology, has been investigated. F_t's near 30 GHz and F_{max}'s from 30 to 40 GHz have been obtained for n-channel devices, while F_t and F_{max} were 13 and 20 GHz, respectively, for the p-channel MOSFETs.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	15 November 1998	Quarterly Technical Summary: 1 August – 31 October 1998

4. TITLE AND SUBTITLE

Advanced Electronics Technology

5. FUNDING NUMBERS

C — F19628-95-C-0002

6. AUTHOR(S)

Charles W. Niessen and David C. Shaver

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lincoln Laboratory, MIT
244 Wood St.
Lexington, MA 02420-9108

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ AF Materiel Command
Wright Patterson AFB, OH 45433-5066

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

ESC-TR-98-043

11. SUPPLEMENTARY NOTES

None

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This Quarterly Technical Summary covers the period 1 August through 31 October 1998. It consolidates the reports of Division 6 (Communications and Information Technology) and Division 8 (Solid State) on the Advanced Electronics Technology Program.

14. SUBJECT TERMS

digital computers	electro-optic devices	submicrometer technology
integrated circuits	materials research	biosensor and molecular technologies
computer systems	laser research	microelectronics
computer network	quantum electronics	analog device technology

15. NUMBER OF PAGES
23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Same as Report